BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/965,916	09/28/2001	Michael D. Ruehle	42390.P11975	4227

8791 7590 08/05/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
DO, CHAT C	

ART UNIT	PAPER NUMBER
2124	

DATE MAILED: 08/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/965,916	RUEHLE, MICHAEL D.	
	Examiner	Art Unit	
	Chat C. Do	2124	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/2801; 11/20/01; 01/15/02; 04/04/02*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7,9-12,15,17-20,23-31 and 33* is/are rejected.

7)☒ Claim(s) *5-6, 8, 13-14, 16, 21-22, and 32* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/20/01;01/27/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4, 7, 9-12; 15, 17-20, 23-31, and 33 are rejected under 35 U.S.C. 102(b) as being anticipated by Weixin et al. ("A Systolic Linear Array for Modular Multiplication").

Re claim 1, Weixin et al. disclose in Figures 2-4 an apparatus comprising: a modular multiplier (title) including a plurality of independent computation channels (e.g. one for C_{in} and one for q_{in}), plurality of independent computation channels (e.g. description of Figure 3 wherein each PE can be used to compute various variables) including a first computation channel and a second computation channel (e.g. one for C_{in} and one for q_{in}); and a coupling device (e.g. control device as seen in Figure 4a as "sel" control with an inverter) interposed between first computation channel and second computation channel to receive a first control signal (e.g. "sel" control signal applied directly to q_{in}) and to couple first computation channel to second computation channel in response to a receipt of first control signal (e.g. "sel" control signal applied actively directly to c_{in} where "sel" is high).

Re claim 2, Weixin et al. further disclose in Figures 2-4 a linear systolic array of processing elements (e.g. description of Figure 2), linear systolic array of processing elements including plurality of independent computation channels (Figure 3).

Re claim 3, Weixin et al. further disclose in Figures 2-4 3 a coupling device comprises a coupling device to receive a second control signal and to selectively couple first computation channel to second computation charmel in response to a state of second control signal (e.g. "sel" control signal in Figure 4a and right column page 173 lines 11-15).

Re claim 4, Weixin et al. further disclose in Figures 2-4 an apparatus having a first mode of operation corresponding to a first state of second control signal wherein first computation channel is operably separated from second computation channel and a second mode of operation corresponding to a second state of second control signal wherein first computation channel is operably coupled to second computation channel via coupling device (e.g. "sel" state is high for computing q_{in} and "sel" state is low for computing c_{in}).

Re claim 7, Weixin et al. further disclose in Figures 2-4 modular multiplier comprises a Montgomery multiplier (abstract).

Re claim 9, it is a processor claim of claim 1. Thus, claim 9 is also rejected under the same rationale as cited in the rejection of rejected claim 1.

Re claim 10, it is a processor claim of claim 2. Thus, claim 10 is also rejected under the same rationale as cited in the rejection of rejected claim 2.

Re claim 11, it is a processor claim of claim 3. Thus, claim 11 is also rejected under the same rationale as cited in the rejection of rejected claim 3.

Re claim 12, it is a processor claim of claim 4. Thus, claim 12 is also rejected under the same rationale as cited in the rejection of rejected claim 4.

Re claim 15, it is a processor claim of claim 7. Thus, claim 15 is also rejected under the same rationale as cited in the rejection of rejected claim 7.

Re claim 17, it is a system claim of claim 1. Thus, claim 17 is also rejected under the same rationale as cited in the rejection of rejected claim 1.

Re claim 18, it is a processor claim of claim 2. Thus, claim 18 is also rejected under the same rationale as cited in the rejection of rejected claim 2.

Re claim 19, it is a processor claim of claim 3. Thus, claim 19 is also rejected under the same rationale as cited in the rejection of rejected claim 3.

Re claim 20, it is a processor claim of claim 4. Thus, claim 20 is also rejected under the same rationale as cited in the rejection of rejected claim 4.

Re claim 23, Weixin et al. further disclose in Figures 2-4 method comprising: receiving a first control signal (e.g. high of "sel" control signal in Figure 4a) and a plurality of operands (e.g. S_{out} and stop); and performing a modular multiplication operation (e.g. abstract) on plurality of operands utilizing a modular multiplier including a plurality of independent computation channels (e.g. description of Figure 1), plurality of independent computation channels including a first computation channel and a second computation channel (e.g. computation of c_{in} and q_{in}), wherein performing modular multiplication operation comprises: coupling first computation channel with second computation channel

in response to receiving first control signal (e.g. "sel" control signal); performing a first portion of modular multiplication operation utilizing first computation channel (e.g. computation of c_{in}); and performing a second portion of modular multiplication operation utilizing second computation channel (e.g. computation of q_{in}).

Re claim 24, it is a method claim and has limitations cited in claim 2. Thus, limitations of claim 24 are also rejected under the same rationale as cited in the rejection of rejected claim 2.

Re claim 25, Weixin et al. further disclose in Figures 2-4 a step of performing a first portion of modular multiplication operation comprises providing plurality of operands to first computation channel and processing plurality of operands utilizing first computation channel to produce an intermediate result (e.g. Figure 2 the output of channel in PE_2 is intermediate result), coupling first computation channel with second computation channel comprises providing intermediate result to second computation channel (e.g. "sel" control signal); and performing a second portion of modular multiplication operation comprises processing intermediate result utilizing second computation channel.

Re claim 26, it is a method claim and has limitations cited in claim 1. Thus, limitations of claim 26 are also rejected under the same rationale as cited in the rejection of rejected claim 1.

Re claim 27, it is a machine-readable medium claim of claim 23. Thus, claim 27 is also rejected under the same rationale as cited in the rejection of rejected claim 23.

Re claim 28, it is a machine-readable medium claim of claim 24. Thus, claim 28 is also rejected under the same rationale as cited in the rejection of rejected claim 24.

Re claim 29, it is a machine-readable medium claim of claim 25. Thus, claim 29 is also rejected under the same rationale as cited in the rejection of rejected claim 25.

Re claim 30, it is a machine-readable medium claim of claim 26. Thus, claim 30 is also rejected under the same rationale as cited in the rejection of rejected claim 26.

Re claim 31, Weixin et al. further disclose in Figures 2-4 a method comprising: receiving a data value at a first end of a systolic array multiplier from a second end of the systolic array multiplier and receiving a data value at the second end from the first end (Figure 2).

Re claim 33, Weixin et al. further disclose in Figures 2-4 a step of processing data in processing elements, which operate on a given problem during alternating cycles of a clock signals (Figure 4b).

Allowable Subject Matter

3. Claims 5-6, 8, 13-14, 16, 21-22, and 32 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. U.S. Patent No. 6,356,636 to Foster et al. disclose a circuit and method for fast modular multiplication.

b. U.S. Patent No. 6,219,815 to Desjardins et al. disclose a high-speed syndrome calculation.

c. U.S. Patent No. 4,799,182 to Marwood discloses a cellular floating-point serial pipelined multiplier.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (703) 305-5655. The examiner can normally be reached on M => F from 7:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chaki Kakali can be reached on (703) 305-9662. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Chat C. Do
Examiner
Art Unit 2124

July 26, 2004

JOHN CHAVIS
PATENT EXAMINER
ART UNIT 2124